

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2001-510970

(P2001-510970A)

(43) 公表日 平成13年8月7日(2001.8.7)

(51) Int.Cl. ⁷	識別記号	F I	ページ* (参考)
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R 5 J 1 0 4
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B 5 K 0 6 7
H 0 4 Q 7/10			6 0 1 A
7/20			6 0 1 E
7/22		H 0 4 Q 7/02	Z
審査請求 未請求 予備審査請求 有 (全 41 頁) 最終頁に続く			

(21) 出願番号 特願2000-503671(P2000-503671)
 (86) (22) 出願日 平成10年7月13日(1998.7.13)
 (85) 翻訳文提出日 平成12年1月17日(2000.1.17)
 (86) 国際出願番号 P C T / G B 9 8 / 0 2 0 6 4
 (87) 国際公開番号 W O 9 9 / 0 4 5 8 3
 (87) 国際公開日 平成11年1月28日(1999.1.28)
 (31) 優先権主張番号 9 7 1 5 0 9 7 . 3
 (32) 優先日 平成9年7月17日(1997.7.17)
 (33) 優先権主張国 イギリス (G B)

(71) 出願人 オレンジ パーソナル コミュニケーションズ サーヴィシーズ リミテッド
 イギリス, プリストール ビーエス12 4
 キュージェイ, アーモンズベリー, グレート パーク ロード, セイント ジェイムズ コート (番地なし)

(72) 発明者 フォード, ビーター
 イギリス, プリストール ビーエス17 5
 アールビー, イェイト, サマーズ ミード 18

(74) 代理人 弁理士 山田 行一 (外2名)

最終頁に続く

(54) 【発明の名称】 セルラー方式通信システムにおける暗号化同報メッセージ

(57) 【要約】

所定のアクセス権を有するユーザ移動局 (8) が、セルラー方式電気通信ネットワーク内の共通のセルチャネルで同報されたメッセージを明瞭に表示できるようにする方法を開示する。メッセージは、同報前に予め定められた暗号化キーを用いて暗号化され、対応する解読キーが対応するアクセス権を有する移動局 (8) に与えられる。適切なアクセス権を欠いた移動局の場合、メッセージが受信されて取り上げられると、そのメッセージは、暗号化形式、すなわち理解できない形式でしか表示されない。同じ共通チャネル上のセル内で同報されるある種のメッセージは、一般アクセスメッセージとみなされる。この種のメッセージは、非暗号化形式で同報され、メッセージが同報されるセルにキャンプオンされた移動局 (8) によって理解可能な形式で表示することができる。

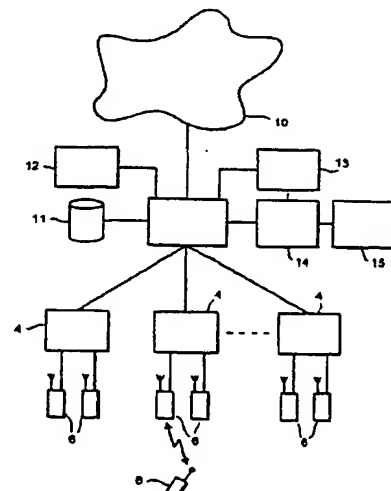


FIG. 1

【特許請求の範囲】

【請求項1】 セルラー方式電気通信ネットワークにおいてユーザに情報を配信する方法であって、前記ネットワークは、移動交換センタと、前記ネットワークの複数のセルにおいて送受信を行う複数の基地局と、を備えており、

複数の移動局を用意するステップであって、前記移動局の各々が、関連付けられた情報アクセスステータスを有しているステップと、

前記ネットワークの少なくとも一つのセルの共通チャネル上で信号を同報するステップであって、前記信号が、前記少なくとも一つのセルにおける一般受信のために、暗号化形式のアクセス制限メッセージを含んでいるステップと、

第1情報アクセスステータスを有する第1移動局が、前記メッセージを解読し、前記セルによりサービスが提供されるときに前記メッセージを非暗号化形式でユーザに提供できるようにするステップと、

第2情報アクセスステータスを有する第2移動局が前記セル内でサービスが提供されるときに前記メッセージを非暗号化形式でユーザに提供することを防止するステップと、
を備える方法。

【請求項2】 前記第1移動局に前記メッセージ用の解読キーが供給される請求項1記載の方法。

【請求項3】 前記解読キーが、複数の移動局のいずれかと関連付けて使用することの可能な着脱自在モジュール内に保持される、請求項2記載の方法。

【請求項4】 前記メッセージが前記着脱自在モジュールで解読される請求項3記載の方法。

【請求項5】 前記信号が、前記メッセージの一部分に付随するパディングデータを含み、この部分が非暗号化形式で前記信号に含まれる、請求項2または3記載の方法。

【請求項6】 前記信号が、メッセージに付随するメッセージ識別子を含むヘッダ部を備えており、前記第1および第2移動局の双方が前記メッセージ識別子を読み取ることができるようにするステップを備えている、請求項1～5のいずれかに記載の方法。

【請求項7】 前記情報アクセスステータスを定義するステータスデータが第1移動局の着脱自在モジュール内に記憶される請求項1～6のいずれかに記載の方法。

【請求項8】 前記ステータスデータが解読キーを含んでいる請求項7記載の方法。

【請求項9】 前記解読キーが前記着脱自在モジュール内に暗号化形式で記憶される請求項8記載の方法。

【請求項10】 前記解読キーが、前記着脱自在モジュールに特有のデータ列を用いて前記第1移動局により解読される、請求項9記載の方法。

【請求項11】 前記データ列が前記セルラー方式電気通信ネットワークで使用される加入者識別子である請求項10記載の方法。

【請求項12】 前記セルラー方式電気通信ネットワーク内で無線インタフェースを介して前記第1移動局に前記ステータスデータを送信するステップを更に備える請求項7～11のいずれかに記載の方法。

【請求項13】 前記信号が、対応するアクセス権を各々が有する複数のアクセス制限メッセージを含んでおり、

前記移動局に前記アクセス権を与えるステップと、アクセス制限メッセージに対応するアクセス権を有する移動局のみが、前記セル内でサービスが提供されるときにユーザにそのアクセス制限メッセージを提供できるようにするステップと、を備える請求項1～12のいずれかに記載の方法。

【請求項14】 前記第1移動局の各々に、各第1移動局に対して保有される加入契約に従って前記アクセス権のなかから選択されたものを提供するステップを備える請求項13記載の方法。

【請求項15】 複数のアクセス制限メッセージタイプの各々に対して暗号化キーを記憶するステップと、その対応メッセージタイプに応じた暗号化キーを用いて前記各アクセス制限メッセージを暗号化するステップと、を更に備える請求項13または14記載の方法。

【請求項16】 複数の加入記録を記憶するステップを備え、前記加入記録の各々が前記アクセス権を定義するアクセス権データを含んでいる請求項13～

15のいずれかに記載の方法。

【請求項17】 加入記録に対する前記アクセス権データを変更して、ユーザが理解可能なように受信することができるアクセス制限メッセージのタイプを変更するステップを備える請求項16記載の方法。

【請求項18】 前記信号が一般アクセスメッセージを含んでおり、前記第1および第2移動局の双方が、前記セル内でサービスが提供されるときに前記一般アクセスメッセージをユーザに提供できるようにするステップを備えている請求項1～17のいずれかに記載の方法。

【請求項19】 前記共通チャネルがGSM型通信システムのセルブロードキャストチャネルである請求項19記載の方法。

【請求項20】 他のアクセス制限メッセージが前記セルラー方式電気通信ネットワークの異なるエリアに位置するセル内で同報される請求項1～19のいずれかに記載の方法。

【請求項21】 セルラー方式電気通信システムにおいて情報を受信する装置であって、

 解読キーを記憶する手段と、

 前記セルラー方式電気通信システムのセルの共通チャネル上で同報されるメッセージを受信する手段と、

 記憶された前記解読キーを用いて前記メッセージを解読する手段と、

 解読された前記メッセージをユーザに対して表示する手段と、

を備える装置。

【請求項22】 前記記憶手段が着脱自在モジュールの一部である請求項21記載の装置。

【請求項23】 前記表示手段は、前記メッセージに対する解読キーが前記記憶手段内に保持されているときに、メッセージを解読された形式で表示し、前記メッセージに対する解読キーが前記記憶手段内に保持されていないときに、前記メッセージを暗号化された形式で表示するように構成されている請求項21または22記載の装置。

【請求項24】 前記解読手段が着脱自在モジュールの一部である請求項2

1、22または23記載の装置。

【請求項25】 セルラー方式移動体電話である請求項21、22、23または24記載の装置。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、GSM (Global System for Mobile communication: 世界移動通信システム) デジタルセルラー方式無線ネットワークなどのセルラー方式電気通信ネットワークにおける情報の配信および受信を行う装置の方法に関する。

【0002】**【従来の技術】**

GSM標準は、欧州電気通信標準化機構 (ETSI) 発行の一組の技術仕様書に定義されている。現在では、GMS標準、およびその変形例 (例えばDCS 1800標準) に従って動作する多くの移動体電気通信ネットワークが存在する。

【0003】

提供される一つのサービスは、セルブロードキャスト (CB) サービスまたはショートメッセージセルブロードキャスト (SMS CB) サービスと呼ばれるサービスである。このサービスでは、テキストページ形式の情報が、ネットワーク内のセルの共通チャネル (セルブロードキャストチャネル、CBCH) で送信される。これらのページの送信は、一定間隔で繰り返される。ユーザは、移動局上でキーを選択操作して情報の検索および表示を行うために、その情報を保存することが可能であり、あるいはその情報を保存しないようにセルブロードキャスト機能をオフにすることができる。この情報は、地域施設 (病院、薬局、タクシー等) のリスト、地域気象予報、地域日時表示など、地域特有の情報を含むように意図されている。

【0004】**【発明が解決しようとする課題】**

しかしながら、現在、セルブロードキャスト機能は、現行GSM型ネットワークおよびそこで使用される移動局で提供されるものの、実際には広く実施されているわけではない。この理由の少なくとも一部は、おそらく、このサービスを介した情報の収集および配布に伴うコストである。

【0005】

【課題を解決するための手段】

本発明のある態様では、セルラー方式電気通信ネットワークにおいてユーザに情報を配信する方法が提供される。ここで、このネットワークは、移動交換センタと、このネットワークの複数のセルで送受信を行う複数の基地局と、を備えている。この方法は、

複数の移動局を用意するステップであって、前記移動局の各々が、関連付けられた情報アクセスステータスを有しているステップと、

前記ネットワークの少なくとも一つのセルの共通チャネル上で信号を同報通信するステップであって、前記信号が、前記少なくとも一つのセルにおける一般受信のために、暗号化形式のアクセス制限メッセージを含んでいるステップと、

第1情報アクセスステータスを有する第1移動局が、前記メッセージを解読し、前記セルによりサービスが提供されるときに前記メッセージを非暗号化形式でユーザに提供できるようにするステップと、

第2情報アクセスステータスを有する第2移動局が前記セル内でサービスが提供されるときに前記メッセージを非暗号化形式でユーザに提供することを防止するステップと、を備えている。

【0006】

本発明のこの態様の利点は、次の通りである。すなわち、情報へのアクセスを許可されていないユーザは、メッセージを暗号化形式でしか見ることができず、内容を理解することができない。一方、情報へのアクセス権を有するユーザは、解読済みの理解可能な形式でメッセージを見ることができる。サービスは、加入契約に基づいて提供することができる。ネットワーク中の一部の加入者は、電気通信ネットワークで提供される他のサービス（音声呼出しサービスなど）に加えてセル内で一般的に同報される情報にアクセスしたいと考えるかもしれない、その場合、セルラー情報同報サービスへのアクセスを可能にする加入契約を申し込むことになる。また、他のユーザは、セル内の情報同報の恩恵を受けたくないと考えるかもしれない、その場合、おそらくは少ない費用で、それらの情報へのアクセスを防ぐ加入契約を申し込むことになる。

【0007】

好ましくは、上記の信号は、対応するアクセス権を各々が有する複数のアクセス制限メッセージを含んでおり、上記の方法は、移動局にアクセス権を与えるステップと、アクセス制限メッセージに対応するアクセス権を有する移動局のみが、セル内でサービスが提供されるときにユーザにそのアクセス制限メッセージを提供できるようにするステップと、を備えている。これにより、ユーザがアクセス可能な情報の種類の選択がユーザ単位で可能となり、加入契約を加入者個々のニーズに適応させることが可能となる。

【0008】

上記の信号は、一般アクセスメッセージを含んでいてもよく、上記の方法は、セル内でサービス提供されるときに第1および第2移動局の双方がユーザにその一般アクセスメッセージを提供できるようにするステップを備えていてもよい。これにより、アクセス制限メッセージおよび一般アクセスメッセージの双方をセルラー方式電気通信システムのセル内での同報により配布することが可能となり、保有する加入タイプにかかわらず、任意のユーザに情報を提供することが可能となる。

【0009】

好ましくは、他のアクセス制限メッセージが、セルラー方式電気通信ネットワークの異なるエリアに位置するセル内で同報される。これにより、メッセージ内の情報を種々の地域に適合させ、サービスの有用性を高めることができる。

【0010】

本発明の別の態様によれば、セルラー方式電気通信システムにおいて情報を受信する装置が提供される。この装置は、

解読キーを記憶する手段と、

前記セルラー方式電気通信システムのセル内の共通チャネルでメッセージを受信する手段と、

記憶された前記解読キーを用いて前記メッセージを解読する手段と、

この解読されたメッセージをユーザに対して表示する手段と、を備えている。

【0011】

この態様は、ユーザが電気通信システム内の一つのセルの共通チャネルでアク

セス制限メッセージを受信し、ユーザの移動局に解読キーが与えられている場合には、解読された形式でその情報を見ることができるようにする装置を提供する。解読キーは、所定の加入タイプを有するセルラーユーザにのみ配布することができる。

【0012】

【発明の実施の形態】

以下では、本発明の実施形態を添付の図面を参照しながら説明する。この実施形態は、単なる例示として記載したものにすぎない。

【0013】

図1は、公衆陸上移動体ネットワーク (public land mobile network: PLMN) と呼ばれる GSM ネットワークを概略的に示している。これ自体は公知であるので、その詳細は省略する。移動交換センタ (mobile switching centre: MSC) 2 は、通信リンクを介して多くの基地局コントローラ (base station controller: BSC) 4 に接続される。BSC 4 は、移動交換センタ 2 からサービスの提供を受ける複数のエリアにわたって地理的に分散される。各 BSC 4 は、一つ以上の基地トランシーバ局 (base transceiver station: BTS) 6 を制御する。この BTS 6 は、BSC から離れた場所に位置し、別の通信リンクを介してその BSC に接続される。各 BTS 6 は、BTS がサービスを提供するエリア内の移動局 8 との間で無線信号の送受信を行う。このようなエリアは、「セル」と呼ばれる。GSM ネットワークには、このようなセルが数多く設けられる。これらのセルは、全ネットワーク領域にわたって連続したカバレッジを与えるように連続しているのが理想的である。無線信号は、多くの別個の通信チャンネルに分けられる。これらの通信チャンネルには、共通チャンネルおよびトラヒックチャンネルが含まれる。トラヒックチャンネルは、特定の移動局とのポイントツーポイント通信 (音声呼出し、データ呼出し等) に使用される。共通チャンネルは、セルがサービスを提供する全ての移動局によって受信され、シグナリングデータおよび／又はメッセージデータを含んでいる。

【0014】

移動交換センタ 2 は、通信リンクを介して、移動通信ネットワーク 10 の残り

の部分における他の移動交換センタや、公衆加入電話網 (public service telephone network: PSTN) 等の他のネットワーク (図示せず) にも接続される。移動交換センタ2には、ホームロケーションレジスタ (home location register: HLR) 11が設置される。HLR11は、各移動局8に対して一意の国際移動体加入者識別子 (international mobile subscriber identity: IMSI) を含む加入者確認データを記憶するデータベースである。IMSIは、移動体国番号 (3桁の十進数)、移動体ネットワーク番号 (2桁の十進数)、および特定ネットワーク内の加入者を識別する移動体加入者番号 (最大10桁の十進数) から構成されている。IMSIは、加入者識別モジュール (SIM) (後述する) 内の移動局にも、他の加入者特有の情報と共に記憶される。

【0015】

移動交換センタには、図示しないビジターロケーションレジスタ (VLR) も設置される。VLRは、そのエリア内の移動局用の加入者確認データを一時的に記憶するデータベースである。

【0016】

更に、MSCは、ネットワーク中でセルブロードキャスト (cell broadcast: CB) メッセージを発信するセルブロードキャストセンタ (cell broadcast centre: CBC) 12、ネットワーク内のポイントツーポイントショートメッセージの転送を処理するショートメッセージセンタ (short message centre: SMC) 13、ネットワーク内の管理機能を実行するネットワーク管理センタ (network management centre: NMC) 14、およびシステム内のワークステーションでの手動入力による顧客加入データの更新などを含む顧客サービス機能を実行する顧客サービスシステム (customer services system: CSS) 15に接続されている。

【0017】

図2に示されるように、移動局8 (より具体的には、セルラー方式移動体無線電話) は、送受信アンテナ16、無線周波数トランシーバ18、スピーカ22およびマイクロホン24に接続された音声CODEC20、プロセッサ回路26およびその関連メモリ28、LCD表示装置30、並びに手動入力ポート (キーパッド

）32を備えている。移動局8は、電気接点35を介して、着脱自在なSIM34に接続される。

【0018】

移動局に接続されたSIM34は、SIMプロセッサ36（例えば、日立H8マイクロプロセッサ）およびSIMメモリ38を有する。SIMメモリ38には、例えば、SIMオペレーティングシステムを含む16キロバイトのマスクプログラムROM38a、データ項目の不揮発性記憶用の8キロバイト読み書きEEPROM38b、および動作中にSIMプロセッサ36によって使用される256バイトRAMが含まれる。

【0019】

上述のように、SIM34は、移動局8のプロセッサ26によるデータ項目の記憶および検索に使用される。移動局プロセッサ26およびSIMプロセッサ36間のインタフェースを介して通信されるデータに関するコマンドセット、データファイル構造およびデータ符号化フォーマットは、すべてGSM技術仕様書11.11に指定されている。

【0020】

図1に示されるネットワーク要素に戻ると、CBC12は、ネットワーク内で同報されるべき一組のセルブロードキャストメッセージを保持し、各メッセージタイプに対して予め定められた位置エリアに従って、これらのメッセージをBSC4に送信する。各セルブロードキャストメッセージには、一意のメッセージ識別子（16ビット整数）が与えられる。この識別子は、メッセージのタイプを特定する。次に、BSC4は、対応するBTS6を介したそのCBCH上でのメッセージ同報に進む。CBCHプロトコルおよび同報のタイミングは、GSM技術仕様書05.02で指定されている。

【0021】

CBC12は、図3に示されるように、暗号化形式で同報すべきメッセージの各タイプに対して暗号化キーを指定するリストを保持する。このキーは、このようなメッセージの各々について、メッセージ識別子に対してリストされる。各キーは16ビット整数であり、メッセージ識別子も16ビット整数であるので、リ

スト内の二つのキーが同一である必要はない。これらのキーは、後述するようにXOR関数を用いてメッセージを暗号化するために使用される。

【0022】

図4は、新しい送信用メッセージをセルブロードキャストメッセージとして受け取るときにCBS12によって実行される手順を示している。新しいメッセージは、例えばCBCに伴うワークステーション上での手動入力によってCBC12内で提供することができ、あるいはリモートソースからオンラインで提供することができる。

【0023】

CBC12が新しいメッセージ（このメッセージは、同一のメッセージ識別子に対して記憶された前のメッセージを更新したものでもよい）を受信すると、このメッセージは、CBC12によって記憶され、同一のメッセージ識別子に対して記憶された前のメッセージは上書きされる（ステップ50）。

【0024】

次に、CBC12は、新しいメッセージが与えられたメッセージ識別子を用いて、図3に示されるキーリストにそのメッセージ識別子が現れているかどうかをチェックする。その特定メッセージ識別子に対してキーが保持されていない場合、このメッセージは、セルブロードキャストによって、メッセージが配信されるセル内でサービスが提供される全ての移動局が一般に利用できるものとなる。このメッセージは、同報通信のために、非暗号化形式で関連BCS4に送信される（ステップ52）。

【0025】

セルブロードキャストメッセージは、一以上のページ（最大15ページ）からなる。各セルブロードキャストページは、88オクテットの情報からなり、この情報は、6オクテットヘッダおよびメッセージテキスト用の82オクテットからなる。最大93文字／ページに等しい7ビットデフォルト文字セットが使用される。

【0026】

図5は、セルブロードキャストメッセージの各ページがCBCH上のBSC／

BTSによりセル内で伝送される方法を示している。この同報通信は、毎ページあたり4ブロックに分割される。第1のブロック100には、ページの通し番号を示す2オクテットのデータ108、ページのメッセージ識別子を示す2オクテットのデータ110、メッセージテキストに使用される符号化方式を特定する1オクテットのデータ112、およびページパラメータを示す1オクテットのデータ114が含まれる。残りの16オクテットのデータ116には、そのページ用のメッセージテキストの第1の部分が含まれる。

【0027】

ページ同報の残りの3ブロック102、104、106は、全体的にメッセージテキストからなる。ただし、各ブロックは、ブロックタイプを示す単一オクテットのデータ118をヘッダとして含んでいる。

【0028】

ブロック部分108で示される通し番号は、特定のメッセージを識別するために使用される16ビット整数である。この通し番号は、所定のメッセージ識別子を有するメッセージが更新されるときに更新される。この通し番号は、12ビットのメッセージコードおよび4ビットの更新番号からなり、これらはメッセージの更新に従って増分される。

【0029】

部分110内のメッセージ識別子は、上述のように、メッセージのタイプを識別するために使用される。

【0030】

部分112に示される符号化方式は、メッセージのソース言語を示すために使用される。これにより、ユーザは、対話不可能な言語で受信されたメッセージを遮断することが可能になる。部分114に示されるページパラメータは、メッセージ内の現在のページ番号およびメッセージ内のページ総数を指定するために使用される。

【0031】

各ページについてのメッセージテキストは、最大93文字からなる。1ページ内のメッセージテキストの長さが93文字より短い場合、パッキングを行って文

字総数を93にするために、復帰(carriage return:CR)文字が使用される。整数のオクテットを維持するため、残りの5ビットは、ページの終端におけるパディングデータとして「0」に設定される。

【0032】

図5に示すブロック構造は、従来のセルブロードキャストメッセージの構造である。この構造は、メッセージが同報されるセルブロードキャストチャネルの受信時に、現在利用可能なGSM型移動局によって受信および表示することができる。

【0033】

再び図4について説明する。CBC12が、キーリスト内で新しいメッセージのメッセージ識別子を検出すると、対応するキーが検索される(ステップ54)。次に、このキーを用いてメッセージの暗号化が行われ(ステップ56)、この後、このメッセージは適切なBSC4に送信される(ステップ58)。ステップ56の暗号化は、次のように行われる。すなわち、キーの最上位8ビットとページ内の各奇数番号メッセージテキストオクテットとの間にXOR関数を適用し、キーの最下位8ビットとページ内の各偶数番号メッセージテキストオクテット(その最後のオクテットを除く)との間にXOR関数を適用することによって暗号化が行われる。

【0034】

暗号化セルブロードキャストメッセージを受信するときにBSC4により同報されるページは、図6に示される形式を有している。各ページは、図5に示される非暗号化ページと同じ構成要素、すなわち、それぞれ様々なヘッダ部を含む四つのブロックからなる。しかしながら、図6において陰影を付けて示すように、メッセージテキストの大部分は暗号化されている。5ビットのパディングデータを含むメッセージテキストの各ページの最終オクテットは、非暗号化のまま残される。これは、暗号化すると失われてしまうパディングデータの完全性を守るためである。また、各ヘッダ部も非暗号化形式で送信される。これにより、全ての移動局8によるヘッダ部のデータの適切な受信および読取りが可能となる。

【0035】

暗号化セルブロードキャストメッセージを適切に受信し、理解可能な形式でユーザに提供するためには、メッセージの暗号化に使用された暗号化キーに対応する解読キーを移動局8に与える必要がある。暗号化関数としてXOR関数を用いると、暗号化／解読プロセスは対称的であり、メッセージの暗号化に使用された同じキーを用いてそのメッセージが解読される。本明細書において、このキーは、データの暗号化に使用される際には暗号化キーと呼ばれ、データの解読に使用される際には解読キーと呼ばれる。

【0036】

移動局8に解読キーを供給するために、遠隔供給手順が使用される。この手順は、欧州特許出願EP-A-0562890（この内容は、参照によって本明細書に組み込まれる）等に記載されているような、移動局8への遠隔SIM更新（remote SIM updating: RSU）メッセージの送信を含み、あるいはGSM技術仕様書11.14、「Specification of the SIM Application Toolkit for the Subscriber Identity Module - Module Equipment (SIM-ME) Interface」に記載されている「SMSポイントツーポイント経由データダウンロード」（SMS-PPデータダウンロード）手順の使用を含んでいる。解読キーは、SIM34での記憶のために、GSM定義ショートメッセージサービス（SMS）等のポイントツーポイントデータ転送プロトコルを用いて、無線インタフェース上を移動局8に送信される。SIM34には、セルブロードキャスト解読キーデータの記憶専用のセルブロードキャスト解読キーデータフィールドが設けられる。

【0037】

図7は、特定加入者がアクセス権を有する各アクセス制限メッセージタイプについての解読キーをその加入者の移動局8に供給するためにNMC14によって実行される手順を示している。CSS15は、その加入者についてのアクセス権を示す記録をその加入者に関して保持している。これらのアクセス権は、加入者がアクセスを持つべきメッセージタイプに対する適切なメッセージ識別子のリストを加入者記録の中に含めることによって示される。このアクセス権リストは、CSS15で更新および変更することができる。

【0038】

加入者の移動局8に供給を行うため、NMC14は、まずCSS15に問合せを行い、加入者に対して保持されているメッセージアクセス権を判定する（ステップ60）。また、NMC14は、加入者のIMSIを検索するため、HLR11にも問合せを行う（ステップ62）。更に、NMC14は、CBC12にも問合せを行い、CSS15から返されるアクセス権の詳細のなかで示される各メッセージ識別子に対応する解読キーを検索する（ステップ64）。次に、CBC12から返される各解読キーは、解読キーの16ビットと加入者のIMSI記録の16個の所定ビットとの間にXOR関数を適用することにより、それ自体が暗号化される（ステップ66）。これは、解読キーを、加入者のIMSI（これは、その加入者のSIM34に記憶されている）にアクセスする移動局8によってしか使用できないようにするためである。

【0039】

解読キーが暗号化されると、NMC14は、無線インタフェースを介してRSUメッセージを加入者の移動局8へのSMSメッセージとして送信するために、RSUメッセージをSMC13に転送する。SMSメッセージは、従来の方法により専用データチャネルを介して移動局8に送信される。RSUメッセージは、図8に示される形式を有しており、ヘッダ部70、加入者がアクセスすべき各メッセージタイプに対するメッセージ識別子、暗号化された解読キー、および各メッセージタイプを容易に識別するために加入者によって使用されるアルファタグ（英数字識別子）を含んでいる。ヘッダ部70は、SMSメッセージがRSUメッセージであることを示すフラグと、メッセージの内容がセルブロードキャスト解読キーデータフィールドに記憶されるべきことを示すコマンドを含んでいる。

【0040】

SMSメッセージを受信すると、移動局は、このメッセージをSMSメッセージとして記憶するためにSIM34に転送する。しかしながら、このメッセージはRSUフラグを有するため、SIMプロセッサ36はメッセージがRSUメッセージであることに注目し、RSUメッセージに含まれるメッセージ識別子、対応する暗号化されたキー、および対応するアルファタグを用いて、SIM34内のセルブロードキャスト解読キーデータフィールドを更新する。このようにして

、セルブロードキャスト解読キーデータフィールドに記憶された識別子に対応するメッセージ識別子を有する全ての暗号化されたセルブロードキャストメッセージを解読する能力が移動局に与えられる。

【0041】

移動局のユーザは、キーパッド32上で適切にキー操作することにより、ユーザによる表示が可能ないように移動局が取得および記憶すべきセルブロードキャストメッセージを選択することができる。また、ユーザは、ユーザが表示を望むアクセス制限メッセージタイプの選択を補助するために、アクセス制限メッセージのメッセージタイプに対するアルファタグを表示させることもできる。更に、ユーザは、一般アクセスメッセージのメッセージタイプに対するメッセージ識別子、および移動局が解読キーを持たないアクセス制限メッセージのメッセージタイプに対するメッセージ識別子も選択することができる。

【0042】

ユーザによる表示が可能ないように選択されるタイプのメッセージ識別子を有するセルブロードキャストメッセージが移動局8によって受信され、そのメッセージ識別子に対して、まだ何らのメッセージも記憶されていない場合、移動局8は、そのメッセージを取得し、SIM34のセルブロードキャストメッセージデータフィールド内に記憶する。SIM34が、セルブロードキャストメッセージ内のメッセージ識別子に対して記憶されたメッセージを既に有している場合、移動局8は、そのメッセージの通し番号をチェックし、更新が行われたかどうかを判断する。更新が行われていれば、移動局は、SIM34内の以前に記憶されたメッセージを更新されたメッセージで上書きする。そうでない場合、移動局8は、セルブロードキャストメッセージの内容を無視する。

【0043】

セルブロードキャストメッセージが新たに取得および記憶されると、ユーザは、例えば音声により、あるいは移動局8のLED表示装置30上の特定のアイコンにより、セルブロードキャストメッセージの表示の準備ができたことを指示するように促される。次に、移動局は、図9に示される手順を実行する。

【0044】

移動局は、まず、メッセージの表示を要求するユーザからの入力を待つ。この入力を受信すると、移動局は、自身が現在そのホームネットワーク（HPLMN）にキャンプオンされているかどうかをチェックする。移動局がそのホームネットワークではないネットワークにキャンプオンされていると、移動局は、記憶されたメッセージの表示に直接進む。そのメッセージが暗号化されている場合、その暗号化メッセージは、ユーザが理解不可能な形で表示される（ステップ78）。これは、そのメッセージがアクセス制限タイプのメッセージであり、他のネットワーク加入者には、その情報へのアクセスが許可されないからである。しかしながら、メッセージが暗号化されていない場合、すなわちメッセージが一般アクセスタイプのメッセージである場合、そのメッセージは、理解可能な形で表示される（ステップ80）。

【0045】

移動局が、そのホームネットワークにキャンプオンされている場合、移動局は、本発明にしたがって供給されたセルブロードキャスト解読キーデータフィールドをSIM34が有しているかどうかをチェックする。セルブロードキャスト解読キーデータフィールドを有していない場合、移動局は、メッセージ同報のアクセスタイプに応じて、もう一度暗号化メッセージの表示に進むか（ステップ78）、理解可能なメッセージの表示（ステップ80）に進む。

【0046】

現在移動局内に位置するSIM34がセルブロードキャスト解読キーデータフィールドを有する場合、移動局は、SIM34への問合せに進み、記憶されたメッセージのメッセージ識別子がセルブロードキャスト解読キーデータフィールドに存在するかどうかをチェックする。存在しない場合、受信メッセージは一般アクセスタイプのメッセージであり、このメッセージは、理解可能な形で移動局8により表示される（ステップ80）。そうでない場合、このメッセージは、ユーザがアクセス権を持たないアクセス制限タイプのメッセージである。この場合、メッセージは、暗号化された形、すなわち理解不可能な形で移動局8により表示され、これにより、ユーザによるそのメッセージ内の情報の受け取りが防止される（ステップ78）。

【0047】

記憶されたメッセージのメッセージ識別子がSIM34上のセルブロードキャスト解読キーデータフィールドに存在する場合、移動局8は、記憶メッセージのメッセージ識別子に対応する被暗号化解読キーを加入者のIMSIと共にSIMから検索する工程に進む（ステップ82）。

【0048】

被暗号化解読キーとIMSIを用いることにより、移動局8は、NMC14で行われる暗号化処理とは逆の処理を実行し、元の解読キーを得る（ステップ84）。この解読は、16ビットの被暗号化解読キーと、暗号化プロセスで使用された加入者IMSIからの所定16ビットからなる同一セットとの間でXOR関数を実行することにより行われる。

【0049】

次に、移動局8は、記憶メッセージの解読に進む。この解読は、暗号化セルブロードキャストメッセージの作成時にCBC12で行われた暗号化処理と逆の処理を実行することにより行われる。すなわち、移動局は、解読キーの8個の最上位ビットと各奇数番号メッセージテキストオクテットとの間でXOR関数を実行するとともに、解読キーの8個の最下位ビットと各偶数番号メッセージテキストオクテット（各ページ内の最終オクテット（もともと暗号化されなかった）を除く）との間でXOR関数を実行する。これにより、元のセルブロードキャストメッセージテキストが復元され、この後、このメッセージテキストは、ユーザが理解可能な形で移動局のLCD表示装置30上に表示される（ステップ88）。

【0050】

図10は、89個のメッセージテキスト文字および4個の復帰（テキストパディング）文字からなるオリジナルセルブロードキャストメッセージの一例を示している。このメッセージは、図4を参照して説明したように暗号化され、移動局によって受信及び記憶された後は、図9に示される手順に従って表示することができる。

【0051】

対応する解読キーが移動局に与えられている場合、このメッセージは、図10

に示されるように元の形で表示される。

【0052】

一方、移動局に適切な解読キーが与えられていない場合、このメッセージは、図11に示されるように擬似ランダム文字セットとして現れる。

【0053】

暗号化キーのビット数は、テキストの符号化において各文字ごとに使用されるビット数に等しくもなければ、その倍数でもないので、元の文字の任意の一つと暗号化されたテキスト内に表示される文字との間に直接の対応はない。この場合、テキスト文字に使用される符号化方式は1文字あたり7ビットを使用し、暗号化キーは16ビットを含んでいる。もちろん、テキスト文字符号化長と暗号化キー長の他の組合せを用いても同様の効果を得ることができる。

【0054】

アクセス制限メッセージに使用される暗号化方法の長期安全性を確保するためには、メッセージテキストを暗号化するために使用される暗号化キーが定期的に変更されることになる。図12は、特定の暗号化キーを更新するためにCBC12によって実行される手順を示している。CBC12は、まず、新しい16ビット暗号化キーをランダムに生成し（ステップ90）、次いで、対象のメッセージ識別子に対して図3に示されるリスト内に以前に記憶された暗号化キーを上書きする（ステップ91）。次に、CBC12は、対象の識別子に対して以前に記憶されたメッセージを検索する工程に進み（ステップ92）、次いで、そのメッセージを新しく生成された暗号化キーで暗号化する工程に進む（ステップ93）。この暗号化処理は、図4を参照して説明したようにメッセージがCBC12によって初めに受信された時に実行されたものと同じであるが、もちろん異なる暗号化キーを使用する。メッセージが暗号化されると、新しいセルブロードキャストメッセージが適切なBSC4に転送される（ステップ94）。これは、BTS6が、対象のBSC4によってサービスが提供されるセル中のセルブロードキャストチャネルを受信する移動局8に向けてCBCH上で同報を行うためである。

【0055】

新しい暗号化キーがCBC12で生成され、対応するセルブロードキャストメ

ッセージが新しく生成されたキーを用いて暗号化されると、同じメッセージタイプへのアクセス権を有するユーザの移動局8に新しい解読キーを与えなければならない。

【0056】

適切な加入者の移動局8にCBC12で生成された新しい解読キーを供給する第1のステップは、図13のように実行される手順である。まず、CSS15は、解読キーが更新されたメッセージのメッセージ識別子のリストをCBC12から受信する(ステップ95)。次に、CSS15は、更新された解読キーリスト上のメッセージ識別子に対する加入記録の記憶を探索する工程に進む(ステップ96)。これは、どの加入契約が更新された解読キーを必要とするかを判断するためである。次いで、CSS12は、このような加入契約のリストを構築する。これらの加入契約はNMC14に転送され、これにより、NMC14が適切な供給手順を実行できるようになる(ステップ97)。この後、NMC14は、CSS15から受信したリストに現れる各加入契約に関して、図7を参照して説明した手順を実行する工程に進む。その結果、このような各加入契約の移動局は、その加入者がアクセスするメッセージタイプに対して、更新された解読キーを含む新しいRSUメッセージを暗号化された形式で受信することになる。これらの解読キーは、新たに生成された暗号化キーを用いて暗号化されたメッセージの解読時に使用するのに適している。

【0057】

上述の実施形態で利用される暗号化／解読機構は、XOR関数の両方向暗号化／解読文字を利用するものであり、多くの種類の情報に関連して使用するにあたって十分に安全である。しかしながら、他の両方向暗号化／解読機構(例えば、対称暗号化／解読キーや公衆／専用の暗号化／解読キーを用いるもの)を利用して、より安全度の高い(あるいは低い)暗号化／解読機構を提供してもよい。

【0058】

上述の実施形態では、一般アクセスメッセージには、暗号化／解読プロセスで使用されるXOR関数は適用されない。しかしながら、「0」の16ビットからなる形の「自由」キーを用いて、このメッセージにXOR関数を適用することも

可能である。この結果、元のメッセージ符号化と同一のメッセージ符号化が行われる。「自由」キーを用いたXOR実行は、一般アクセスメッセージの「暗号化」の際にCBC12で行われ、かつ／または一般アクセスメッセージの「解読」の際に移動局8によって行われてもよい。実際には、暗号化または解読は行われない。

【0059】

上述の実施形態では、移動局8がセルブロードキャストメッセージテキストの解読を実行する。これには、現存する移動局タイプに関連して、移動局自体をカスタマイズする必要がある。これは、移動局が、暗号化されたセルブロードキャストメッセージを普通テキスト形式で提供できるようにするためである。別の実施形態では、GSM技術仕様書11.14に記載されているようなSIMツールキットをサポートするGSM（フェーズ2+）移動局などの標準移動局を使用してもよい。この実施形態では、暗号化されたセルブロードキャストメッセージを解読する機能がSIM34自体に含まれている。このSIM34は、SIMツールキットにより使用可能とされる。

【0060】

繰返しを避けるため、図3、4、7、8、12および13の各々に関して説明した機能は、図13に関して等しく適用するものとする。本実施形態は、最初に述べた実施形態と主に次の点で異なる。すなわち、図6に示される特別なセルブロードキャスト符号化方式は必要でなく、その代わりに従来の「SMS-CB経由データダウンロード」符号化方式が使用される。また、図9に示される手順が移動局によって実行されず、その代わりに移動局は、「SMS-CB経由データダウンロード」メッセージをSIMに直接引き渡し、続いて、SIM（このSIMはプロアクティブである）の指示により、暗号化形式で受信したセルブロードキャストメッセージの普通テキストバージョンを表示する。

【0061】

図4に関して、この実施形態では、任意の適切な種類の暗号化技術をステップ56で 사용할 ことができる。これは、前述のXOR関数であってもよいし、DES、RSA等、他の暗号化技術であってもよい。

【0062】

図6に示される符号化方式の代わりに、本実施形態では、暗号化されたセルブロードキャストメッセージを同報するBSC4の各々が、その暗号化メッセージを「SMS-CB経由データダウンロード」メッセージとしてフォーマットする。この暗号化メッセージは、そのメッセージの暗号化に使用されたキー用の識別子と共にセルブロードキャストページに含まれる。セルブロードキャストメッセージは、セルブロードキャストページに含まれる内容の種類を指定するセルブロードキャストメッセージ識別子と、メッセージタイプが「SIMデータダウンロード」であることを示す転送識別子とを含む。

【0063】

解読キー専用のフィールド（これは、上述したようなRSU手順によって埋められる）に加え、SIM34は、GSM技術仕様書11.11に記載されるようなデータダウンロード用セルブロードキャスト識別子（Cell Broadcast Message Identity for Data Download: CBMID）データフィールドを含んでいる。このデータフィールドは、加入者がその移動局8で受け取りたいと考えるメッセージ内容タイプを識別するデータを保持する。更に、SIM34には、解読と移動局8の表示装置の制御を実行するアプリケーションプログラムも含まれる。このアプリケーションプログラムは、例えば、SIM上のROMまたはEEPROMに格納することができる。

【0064】

移動局がセルブロードキャストダウンロードメッセージを受信すると、移動局8は、まずSIMのCBMIDデータフィールドに問合せを行い、セルブロードキャストメッセージに関して受信されたメッセージIDが、加入者によって、または加入者のために現在選択されているかどうかを判断する。対応するエントリがCBMIDデータフィールド内で発見されると、移動局8は、「SIMへのセルブロードキャストダウンロード」コマンドを用いてSIM34にセルブロードキャストページを透過的に引き渡す。

【0065】

SIM34がセルブロードキャストダウンロードコマンドを受け取ると、SI

Mは、セルブロードキャストページの少なくとも一部の内容を分析することになる。これにより、セルブロードキャストページが暗号化されたメッセージを含んでいるかどうか判断される。暗号化メッセージを含んでいる場合、専用解読キーフィールドに記憶された適切な解読キーを用いてメッセージを解読するために、記憶プログラムが呼び出される。メッセージが解読されると、SIMは、その普通テキストメッセージを「テキスト表示」コマンドで移動局に引き渡す。これに応じて、移動局8は、その普通テキストメッセージを表示する。

【0066】

暗号化メッセージの解読および移動局8に指令して普通テキストメッセージを表示させることに加えて、SIMアプリケーションプログラムは、セルブロードキャストメッセージ中で受信したデータに応じて他の処理を実行してもよい。この処理としては、例えば、CBMIDデータフィールドの内容を更新し、移動局8が受信および処理すべき新しいメッセージ種類を加入者に代わって選択することなどが挙げられる。

【0067】

本実施形態では、加入者が普通テキスト形式のアクセス制限メッセージの受信を許可されていない場合、SIMは、このメッセージ用の適切な解読キーを含んでいなくてもよいし、あるいはネットワークオペレータによって少なくとも一時的に、上記手順を実行しないように構成されていてもよい。上記手順の代わりに、SIMは、様々な別の方法において機能することができる。例えば、SIMが移動局8に指令を出して、メッセージを暗号化形式でユーザに提供させ、またはアクセス拒否メッセージを表示させてもよいし、それでもなお加入者によって選択される種類の暗号化メッセージを含むセルブロードキャストメッセージに応答して、単純に移動局上にいかなる表示も行わないようにしてもよい。

【0068】

従って、暗号化セルブロードキャストメッセージの供給および処理機能は、移動体通信ネットワーク内およびSIM34上に完全に含めることができ、標準（例えば、GSMフェース2+）ハンドセットを改造なしで使用することができる。

【0069】

上記実施形態に関しては、様々な修正および変形を加えることができる。

【0070】

R S Uタイプのショートメッセージを用いて、移動局にエアインタフェースを介して解読キーを供給することは、以下の点で有効である。すなわち、移動局8のS I M 3 4に解読キーを供給するにあたって、加入者側では何らの動作も必要ないことである。しかしながら、解読キー（好ましくは、上述のように加入者のI M S I等を用いて暗号化されたもの）を他の方法（例えば、郵送）でユーザに送ってもよい。移動局8の他の機能により、暗号化された解読キーを手動で移動局に入力し、S I M 3 4内のセルブロードキャスト解読キーデータフィールドに記憶することが可能になる。

【0071】

前記の機構に代わって、他の情報アクセス防止機構を使用することもできる。例えば、移動局上の解読機能や移動局上のセルブロードキャスト受信機能の遠隔許可／禁止が挙げられる。

【0072】

上記実施形態において、S I M 3 4は、移動局8に電気接続されたモジュールの形態をとっている。しかし、S I Mは、無線リンクを介して移動局との間でデータ伝送を行う非接触スマートカードなど、全く独立のモジュールとして実現してもよい。

【0073】

最後に、上記実施形態は、G S Mタイプのネットワークで利用される方法および装置に関するものであるが、T D M A、C D M A、または他の種類の無線インタフェースプロトコルを使用して、他の種類のセルラー方式電気通信ネットワークで本発明を実現できることは言うまでもない。

【0074】

本発明の範囲から逸脱することなく、更なる修正や変形を加えることが可能である。

【図面の簡単な説明】

【図 1】

セルラー方式電気通信システムを概略的に示すブロック図である。

【図 2】

セルラー方式電気通信移動局を概略的に示すブロック図である。

【図 3】

本発明に係るセルブロードキャストセンタに記憶されたりストを示す図である。

【図 4】

本発明に係るセルブロードキャストセンタが実行する機能を示すフローチャートである。

【図 5】

本発明に係るセル内のデータブロック同報通信を示す図である。

【図 6】

本発明に係るセル内のデータブロック同報通信を示す図である。

【図 7】

本発明に係るネットワーク管理センタが実行する機能を示すフローチャートである。

【図 8】

本発明に係る移動局に送信されるショートメッセージを示す図である。

【図 9】

本発明に係るセルブロードキャストメッセージを表示する時に移動局が実行する機能を示す図である。

【図 10】

本発明に係る解読メッセージの表示例を示す図である。

【図 11】

本発明に係る暗号化メッセージの表示例を示す図である。

【図 12】

本発明に従って実行される暗号化キー更新手順を示すフローチャートである。

【図 13】

本発明に従って実行される暗号化キー更新手順を示すフローチャートである。

【図1】

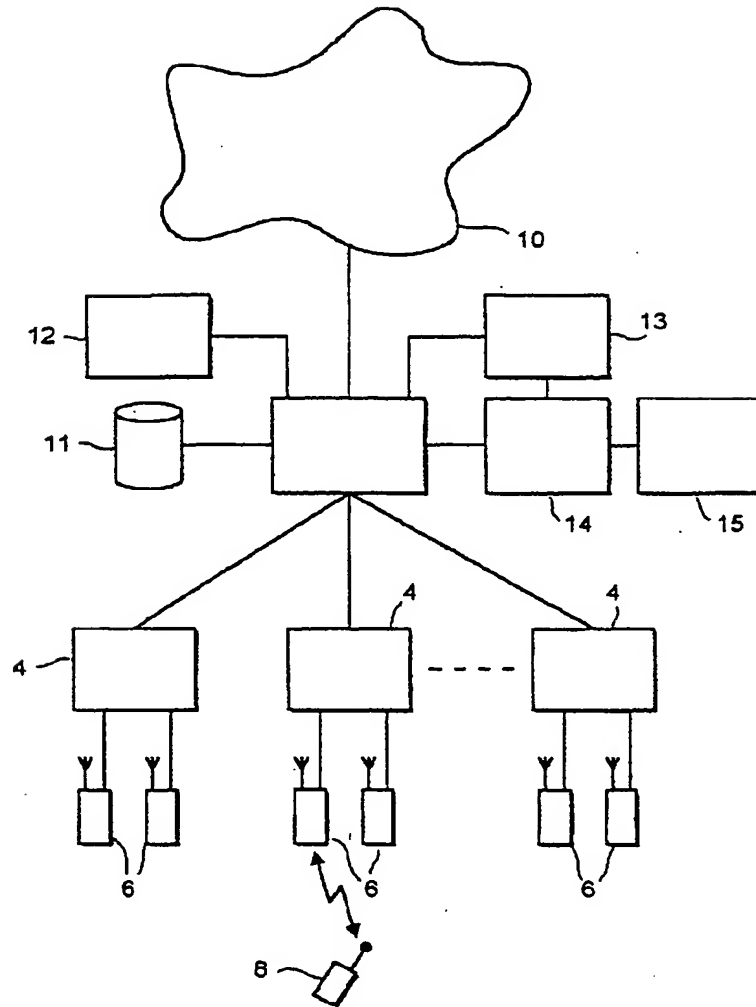


FIG. 1

【図2】

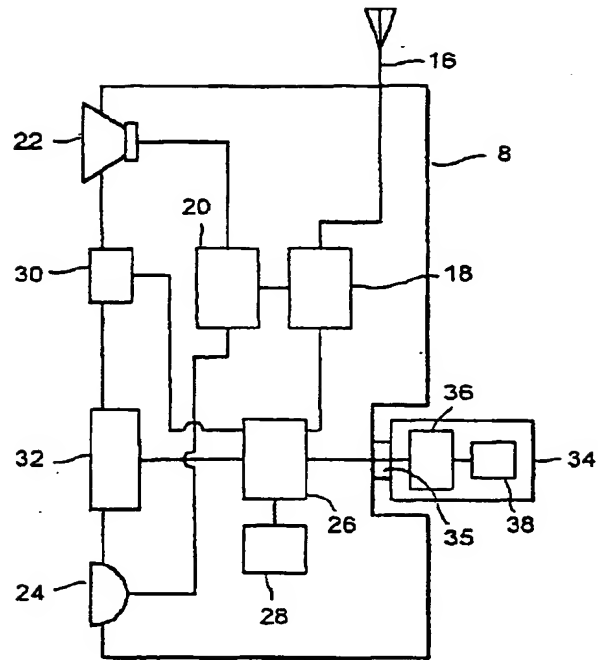
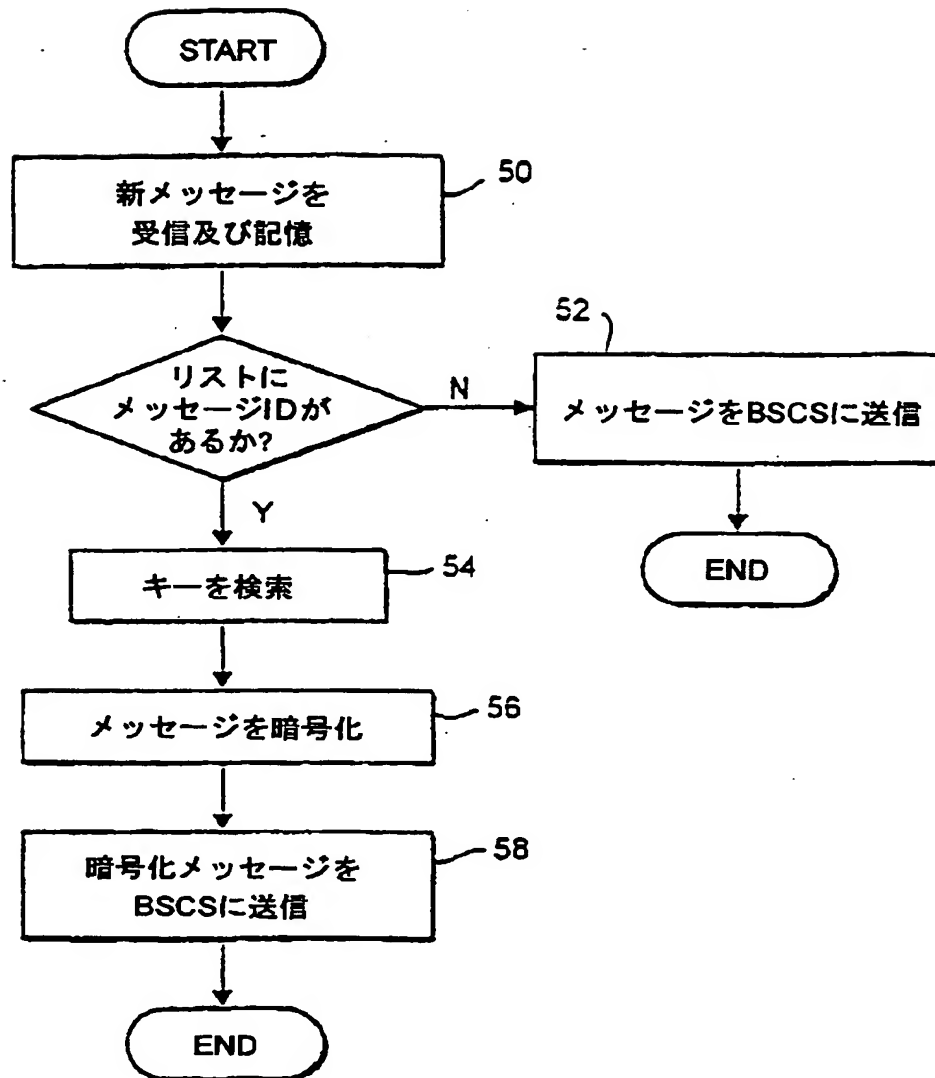


FIG. 2

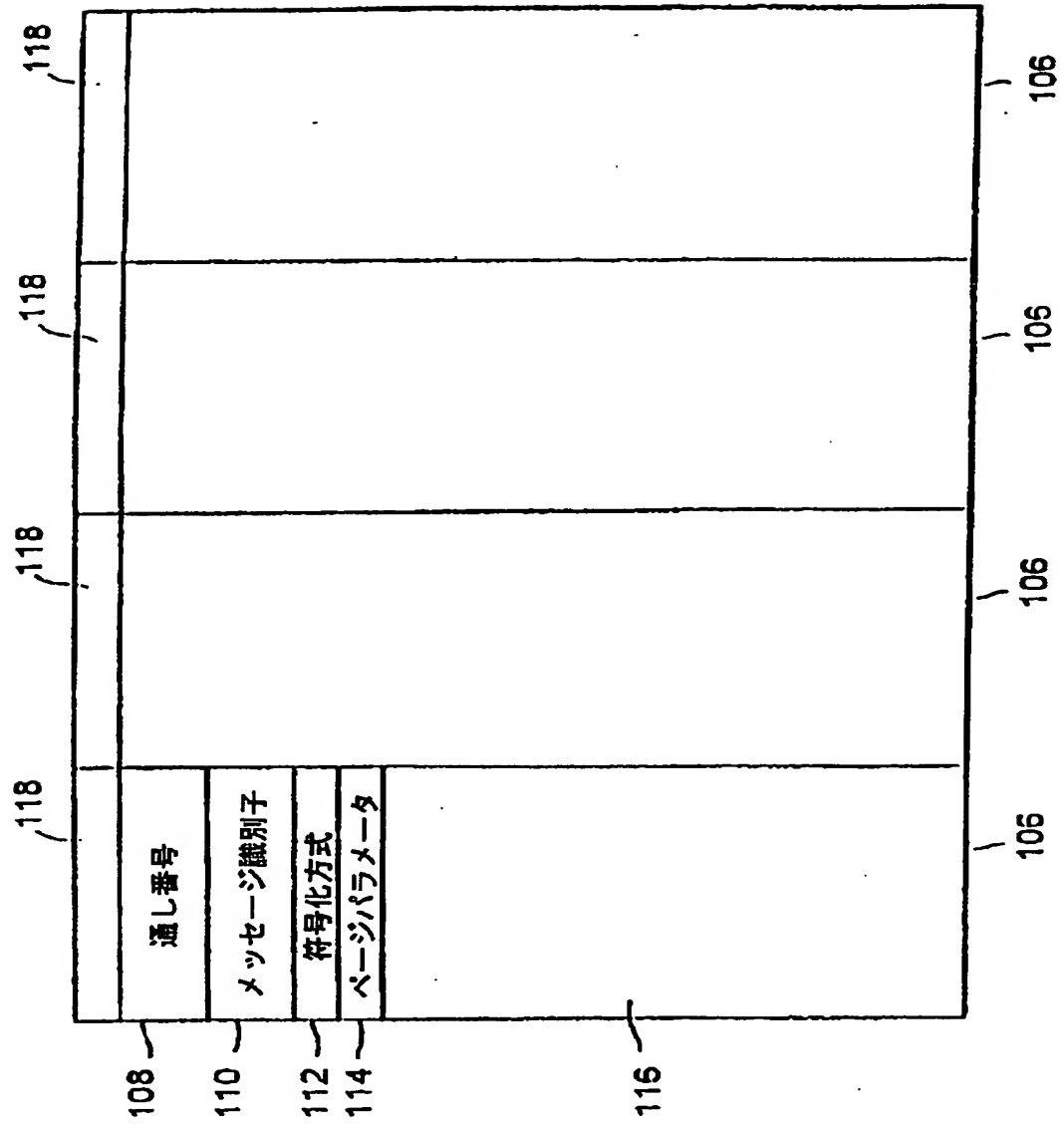
【図3】

メッセージ識別子	キー
.....
.....
• • •	• • •
.....

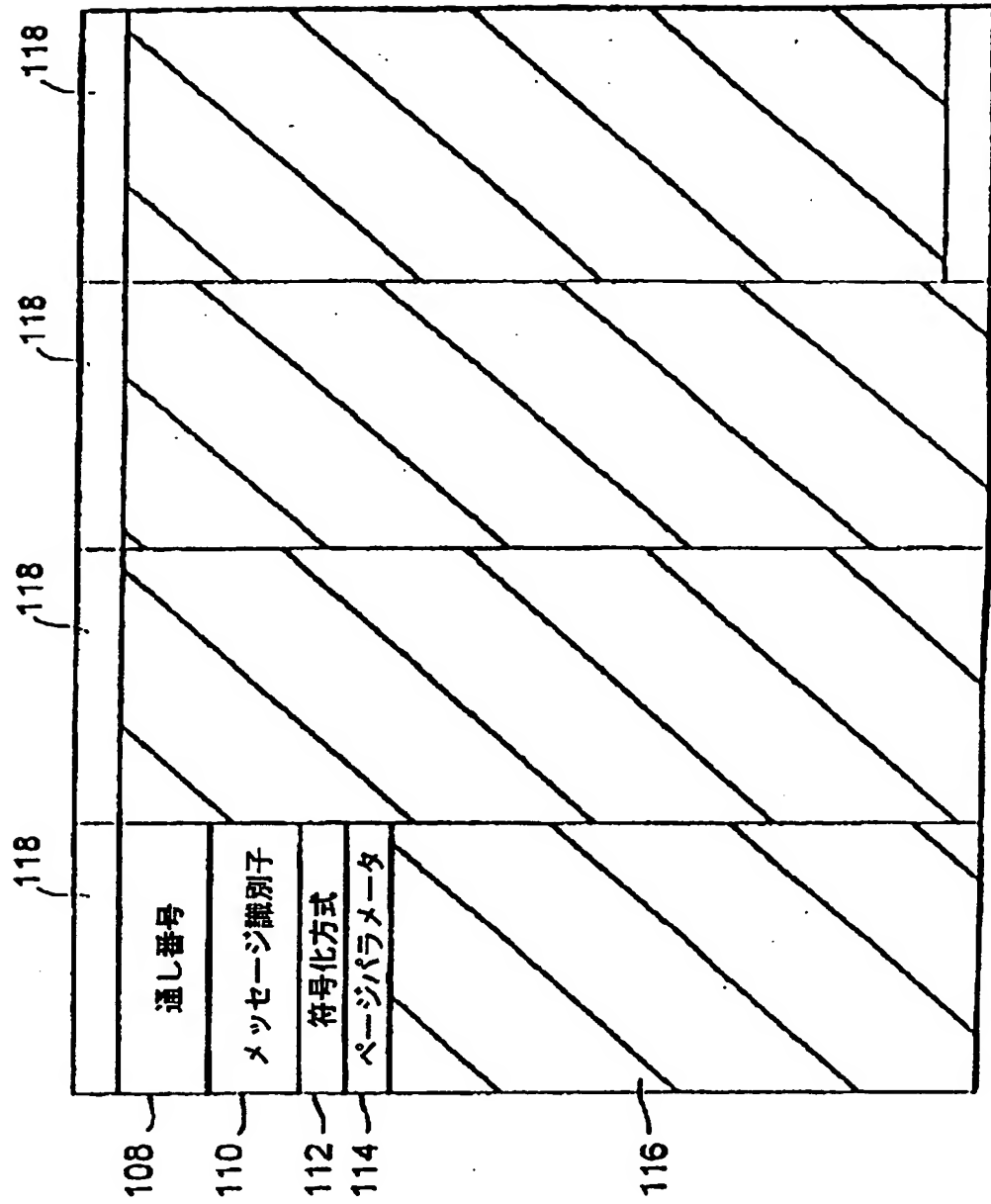
【図4】



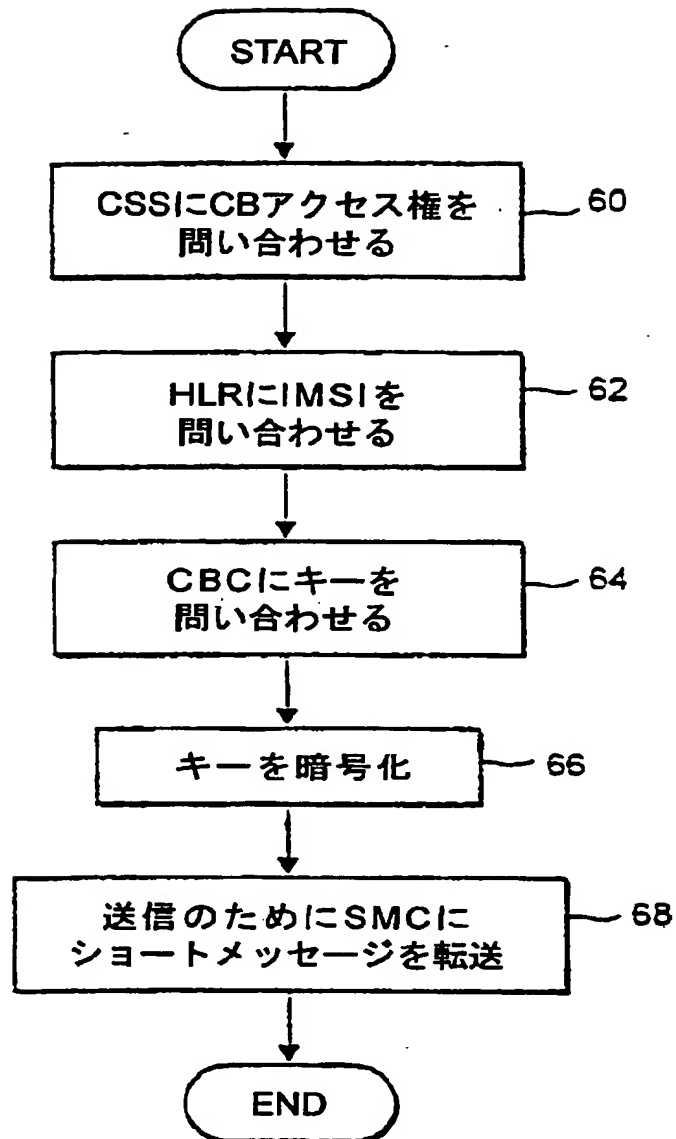
【図5】



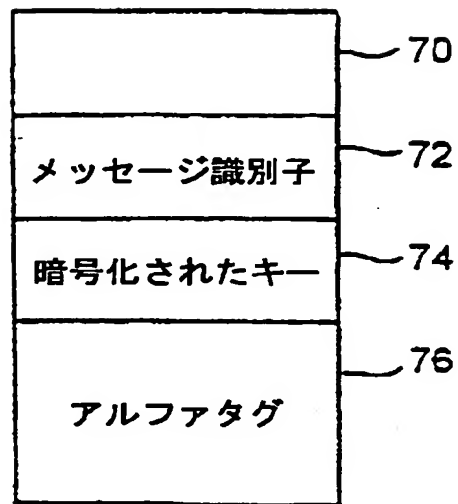
【図6】



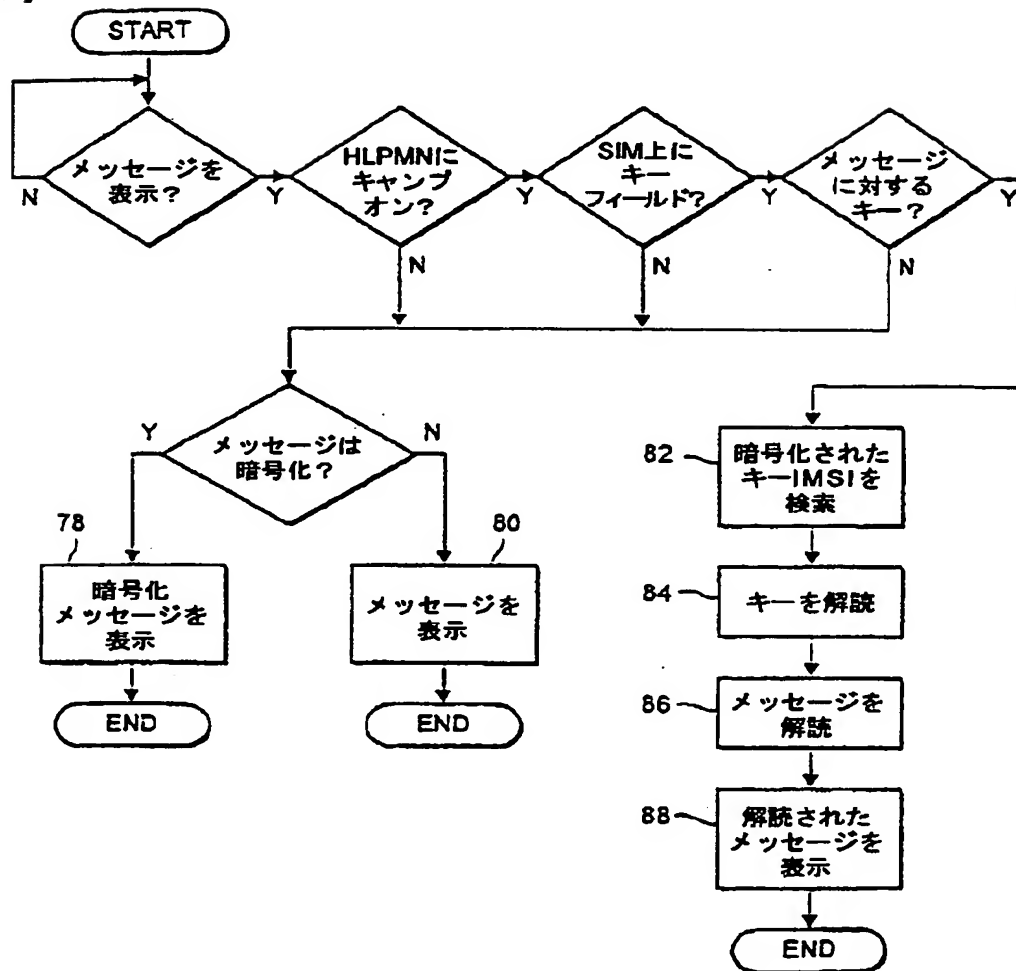
【図7】



【図8】



【図9】



【図10】

T	h	i	s		i	s		a	n		e	x	a	m	p	i	e		o	f		h	o	w		S	M	S		
C	B		m	e	s	s	a	g	e	s		s	h	a	i	i		b	e		c	o	d	e	d	.	C	a	i	
I		"	0	4	5	4	6	2	4	8	2	3	"		F	o	r		m	o	r	e		i	n	f	o	.	CR	
CR		CR	CR																											

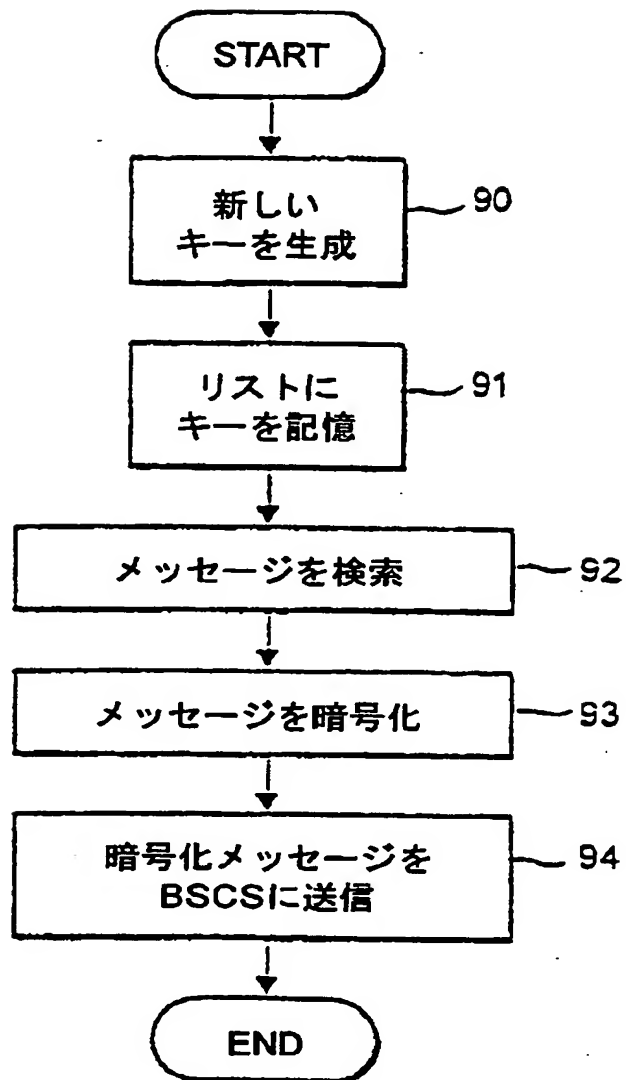
FIG. 10

【図11】

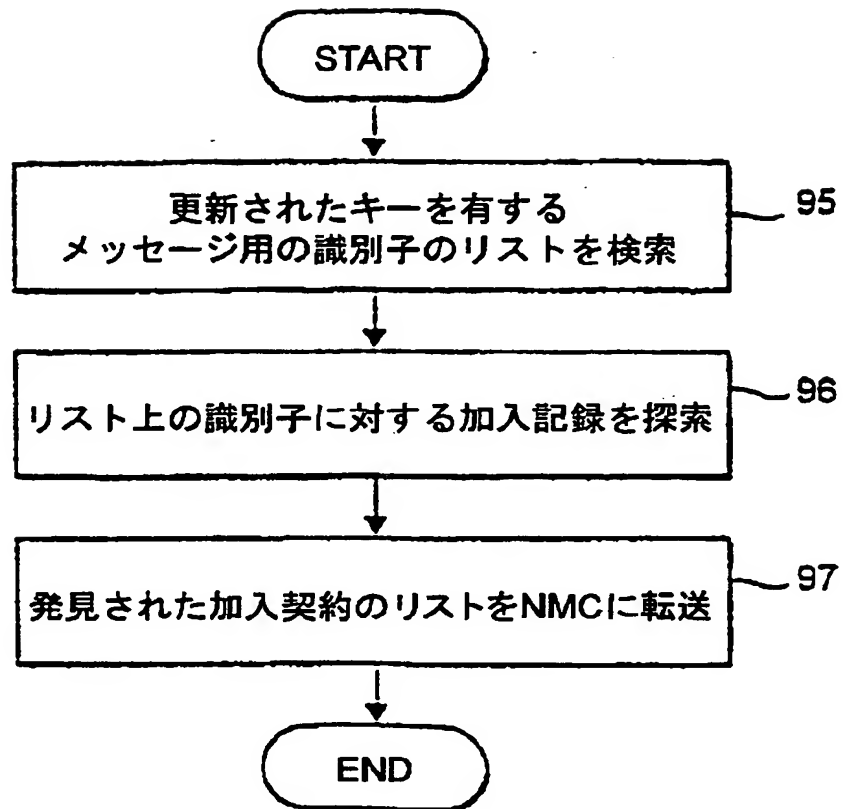
0	s	ü	æ	ö	p	@	f	,	u	ψ	φ	□	x	β	π	ι	ü	ψ	ε	:	0	NU	φ	:	:	d	#	á	0
0	□	m	v	R	æ	/	X	Δ	≠	>	:	F	ü	=	U		6	/	ü	ψ	CR	3	N	Δ	\$	b	X	V	\$
0	ü	Q	V	y	0	≠	X	n	CR	K	V	ü	9	ψ	ö	3	K	S	φ	"	I	R	N	5	W	Ω	φ	C	
:	c	\$																											

FIG. 11

【図12】



【図13】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/GB 98/02064

A. CLASSIFICATION OF SUBJECT MATTER IPC 6 H04Q7/22 H0407/32		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC 6 H04Q		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 41493 A (ERICSSON TELEFON AB L M) 19 December 1996	1, 2, 6, 13-16, 18-21, 25
Y	see page 40, line 5 - page 41, line 2 see page 52, line 20 - page 53, line 17 see page 55, line 10 - line 17 see page 57, line 19 - page 58, line 6 see claims 1-10 --- -/-	3, 7, 8, 12, 17, 22
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" documents referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" documents of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "A" document member of the same patent family		
Date of the actual completion of the international search		Date of making of the international search report
10 November 1998		18/11/1998
Name and mailing address of the ISA European Patent Office, P.B. 6818 Patentlaan 2 NL - 2260 HV Rijswijk Tel. (+31-70) 340-2000, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016		Authorized officer
		Baas, G

Form PCT/ISA/210 (second sheet) (July 1992)

page 1 of 2

INTERNATIONAL SEARCH REPORT

Inter. Appl. No.
PCT/GB 98/02064

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of documents, with indication, where appropriate, of the relevant passages	Relevance to claim No.
Y	FARRUGIA A J ET AL: "SMART CARD TECHNOLOGY APPLIED TO THE FUTURE EUROPEAN CELLULAR TELEPHONE ON THE DIGITAL D-NETWORK" SELECTED PAPERS FROM THE SECOND INTERNATIONAL SMART CARD 2000 CONFERENCE, 4-6 OCTOBER 1989, AMSTERDAM, NL, 1 January 1989, pages 95-107, XP000472724 see page 100, line 1 - page 103, line 21	3,7,8, 12,22
Y	US 5 371 493 A (SHARPE ANTHONY K ET AL) 6 December 1994 see column 3, line 3 - line 10 see column 6, line 35 - line 42	17
A	EP 0 689 368 A (PTT GENERALDIREKTION) 27 December 1995	

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No
PCT/GB 98/02064

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9641493 A	19-12-1996	US 5768276 A AU 6020296 A	16-06-1998 30-12-1996
US 5371493 A	06-12-1994	DE 69219991 D DE 69219991 T EP 0538933 A JP 5218946 A SG 48347 A	03-07-1997 27-11-1997 28-04-1993 27-08-1993 17-04-1998
EP 0689368 A	27-12-1995	AT 153206 T AU 691271 B AU 2174595 A BR 9508091 A CA 2152215 A WO 9535635 A CN 1128476 A CZ 9603513 A DE 59402759 D DK 689368 T ES 2103557 T FI 965078 A GR 3023908 T HU 76397 A JP 8265843 A NO 965315 A NZ 287390 A PL 317643 A SG 34235 A SI 9520064 A SK 161396 A ZA 9505091 A	15-05-1997 14-05-1998 04-01-1996 12-08-1997 21-12-1995 28-12-1995 07-08-1996 14-05-1997 19-06-1997 08-12-1997 16-09-1997 17-12-1996 30-09-1997 28-08-1997 11-10-1996 18-02-1997 19-12-1997 14-04-1997 06-12-1996 30-04-1997 05-11-1997 10-04-1996

フロントページの続き

(51)Int.Cl. ⁷	識別記号	FI	テーマコード(参考)
H 0 4 Q	7/24	H 0 4 Q	A
	7/26		
	7/30		

(81)指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW

Fターム(参考) 5J104 AA16 BA03 EA06 EA18 JA03
NA01 NA02 NA36 NA41
5K067 AA00 BB04 CC04 CC14 DD17
EE16 EE22 HH21 HH36 KK13
KK15